Détection d'intrusions dans les réseaux de capteurs sans fil

Kaci Bader

Rapport de stage

Master Recherche 2 en Informatique
IFSIC-Rennes 1
Année universitaire 2009/2010

Détection d'intrusions dans les réseaux de capteurs sans fil

Auteur : Kaci BADER — **Equipe SERES**
Encadrant : Nora Cuppens et Frédéric Cuppens — **Télécom Bretagne**

Remerciements

Je tiens à exprimer mes plus sincères remerciements à mes encadrants Frédéric et Nora Cuppens, pour avoir encadré ce travail ; je les remercie pour leur disponibilité, leurs encouragements et pour leurs conseils tout au long de ce stage.

Ma reconnaissance va aussi à Fabien Autrel et Joaquin Garcia-Alfaro, pour leur aide, leur compréhension et leurs conseils.

Ma gratitude va également aux membres de la fondation Michel Métivier pour l'aide financière accordée cette année.

Table de matières

Liste des figures

Liste des tableaux

Liste des Acronymes

CRIM	**C**orrélation et **R**econnaissance d'**I**ntentions **M**alveillantes
ESH	**É**conomie et **S**ciences **H**umaines.
IASC	**I**ntelligence **A**rtificielle et **S**ciences **C**ognitives
IDMEF	**I**ntrusion **D**etection Exchange **F**ormat
SDI	**S**ystème de Détection d'Intrusion

LAMBDA	**L**anguage to **M**odel a **D**atabase for **D**etection of **A**ttacks
LUSSI	**L**ogique des **U**sages .**S**ciences **S**ociales et sciences de l'**I**nformation
RCSF	**R**éseau de **C**apteurs **S**ans **F**il
SB	**S**tation de **B**ase
SERES	Sécurité des Réseaux et des Systèmes d'Information
WSN	**W**ireless **S**ensor **N**etwork

Introduction Générale

Au cours de ces dernières années, le développement technologique des réseaux de communication sans fils, a connu un essor important grâce aux avancées technologiques dans divers domaines, telles que la micro-électronique et la miniaturisation. C'est ainsi que de nouvelles voies d'investigation ont été ouvertes avec l'émergence des réseaux de capteurs sans fil.des réseaux à hôtes autonomes et à infrastructure non prédéfinie utilisés dans des domaines très variés tels que la détection de flux de radiation ou; le suivi d'objets en déplacement et leur positionnement.

Les réseaux de capteurs sont composés d'un nombre important de petits appareils opérant de façon autonome et communicant entre eux via des transmissions à courte portée.

Les nœuds capteurs sont conçus pour être déployés d'une manière dense dans des endroits hostiles et difficiles d'accès, d'où la nécessité de limiter au maximum leurs dimensions physiques qui s'obtiennent impérativement au détriment des capacités de calcul, de traitement et de ressources énergétiques.

En raison de leur déploiement en environnements ouverts, de leurs ressources limitées, et la nature broad-cast du medium de transmission, les réseaux de capteurs doivent faire face à de nombreuses attaques. Sans mesures de sécurité, un agent malveillant peut lancer plusieurs types d'attaques qui peuvent nuire au travail des réseaux de capteurs sans fil (RCSF) et empêcher leur bon objectif de déploiement. La sécurité est donc une dimension importante pour ces réseaux.

Des mécanismes de protection existent mais il est souvent nécessaire d'ajouter à ces systèmes des mécanismes de détection d'intrusion afin de compléter les fonctions de sécurité.

Le reste de ce rapport est organisé comme suit : dans la première section, nous présentons le laboratoire et l'entreprise d'accueil. Dans la seconde section nous introduisons l'état de l'art des réseaux de capteurs sans fil. La troisième section est consacrée à la détection d'intrusion. La quatrième section expose les approches de corrélation d'alertes ainsi que le module CRIM et ses fonctions. Dans la cinquième section, nous proposons une architecture de détection d'intrusion et de corrélation d'alertes dans les réseaux de capteurs sans fil. Un scénario d'attaque dans ces réseaux implémenté dans CRIM est décrit dans la sixième section. Nous concluons ce rapport par quelques perspectives de travail là où nous proposons des attaques qui peuvent êtres corrélées en des scénarios complexes dans les réseaux de capteurs sans fil, et nous terminons par une conclusion générale.

1. Présentation du laboratoire d'accueil et de l'équipe

1.1. Présentation de Telecom Bretagne

Télécom Bretagne est, à la fois, une grande école généraliste et un centre de recherche international en sciences et technologies de l'information. Elle s'appuie, pour l'ensemble de ses activités, sur un corps professoral permanent de quelques 150 personnes travaillant au sein de 9 départements d'enseignement-recherche.

Membre de l'Institut Télécom avec Télécom ParisTech, Télécom SudParis, Télécom Lille, Télécom Ecole de Management ,et Eurocom. Télécom Bretagne est un partenaire privilégié des entreprises innovantes et contribue significativement au développement économique régional.

Télécom Bretagne est membre fondateur de l'Université européenne de Bretagne.

1.2. Départements

Télécom Bretagne est composée de 9 départements

- Informatique.
- Electronique.
- Image et traitement de l'information.
- Langue et culture internationales.
- Logique des usages .Sciences sociales et sciences de l'information.
- Micro-ondes.
- Optique.
- Réseaux et sécurité multimédia.
- Signal et Communication

1.2.1.Département LUSSI

- **Présentation**

Le département LUSSI est né en 2004 de la fusion des anciens départements IASC (Intelligence Artificielle et Sciences Cognitives) et ESH (Économie et Sciences Humaines). Réparti sur deux sites, Brest et Rennes, le département LUSSI constitue une véritable équipe pluridisciplinaire : mathématique, informatique, intelligence artificielle, aide à la décision, économie, droit et sociologie.

- **Equipe SERES :**

Le projet SERES (Sécurité des Réseaux et des Systèmes d'Information) s'intéresse aux mécanismes visant à assurer la protection contre des malveillances internes ou externes ainsi qu'aux techniques permettant de détecter ces malveillances.

Les thèmes étudiés concerneront plus particulièrement les points suivants :

- Expression de besoins, politiques et propriétés de sécurité,
- Protection des réseaux et des applications réparties,
- Analyse de vulnérabilités et détection d'intrusion.

Les activités menées dans le cadre de ce projet sont de type :

- Modélisation et formalisation des concepts,
- Conception, développement et validation d'architectures et de logiciels sûrs et d'outils pour administrer la sécurité,
- Expérimentation et évaluation de ces architectures, logiciels et outils.

2. Etat de l'art sur les RCSF

Cette section présente l'état de l'art des réseaux de capteurs, elle consiste a décrire un nœud capteur et ses composants, l'architecture de communication dans les RCSF, leurs caractéristiques, et leur domaines d'application.

2.1. Les capteurs sans fil

Un capteur est un petit appareil autonome capable d'effectuer des mesures simples sur son environnement immédiat, comme la température, la vibration, la pression, etc. Chaque capteur assure trois fonctions principales : la collecte, le traitement et la communication de l'information vers un ou plusieurs points de collecte appelés station de base (SB).Il est constitué de quatre unités principales [1] [2] (voir figure1):

- **Unité de capture (*Sensing unit*)** : elle est composée d'un dispositif de capture physique qui prélève l'information de l'environnement local et un convertisseur analogique/numérique appelé ADC (*Analog to Digital Converter*) qui va convertir l'information relevée et la transmettre à l'unité de traitement.

- **Unité de traitement (*Processing unit*)** : est composée de deux interfaces, une interface pour l'unité d'acquisition et une autre pour l'unité de transmission. Cette unité est également composée d'un processeur et d'une mémoire. Elle acquiert les informations en provenance de l'unité d'acquisition et les stocke en mémoire ou les envoie à l'unité de transmission.

- **Unité de transmission (*Transceiver unit*)** : elle est composée d'un émetteur/récepteur (module radio) pour assurer toutes les émissions et réceptions de données.

- **Unité d'énergie (*Power unit*)** : elle est responsable de la gestion de l'énergie et de l'alimentation de tous les composants du capteur. Elle consiste, généralement, en une batterie qui est limitée et irremplaçable, ce qui rend l'énergie comme principale contrainte pour un capteur.

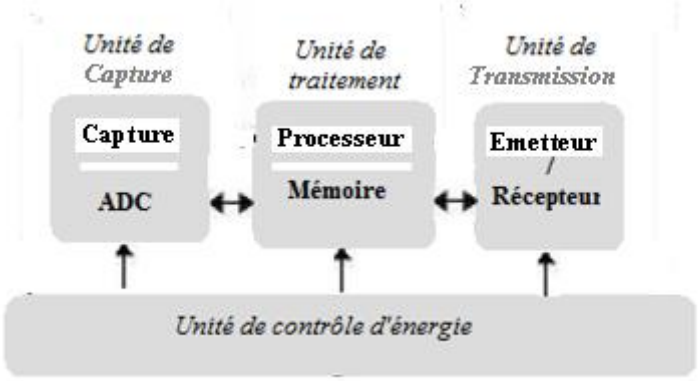


Figure 1:Les composants d'un nœud capteur .

2.2. Définition d'un réseau de capteurs

Un réseau de capteurs est un type spécial de réseau ad hoc où l'infrastructure de communication et l'administration centralisée sont absentes [3] : il est constitué d'un ensemble de dispositifs très petits, nommés nœuds capteurs dispersés dans une zone géographique appelée champs de captage. Chacun de ces nœuds a la capacité de collecter les données, les router vers la station de base (le nœud puits), et par la suite vers l'utilisateur final via une communication multi-sauts. Le nœud puits peut communiquer avec le nœud coordinateur de tâches (utilisateur) par internet ou par satellite [4] (figure2).

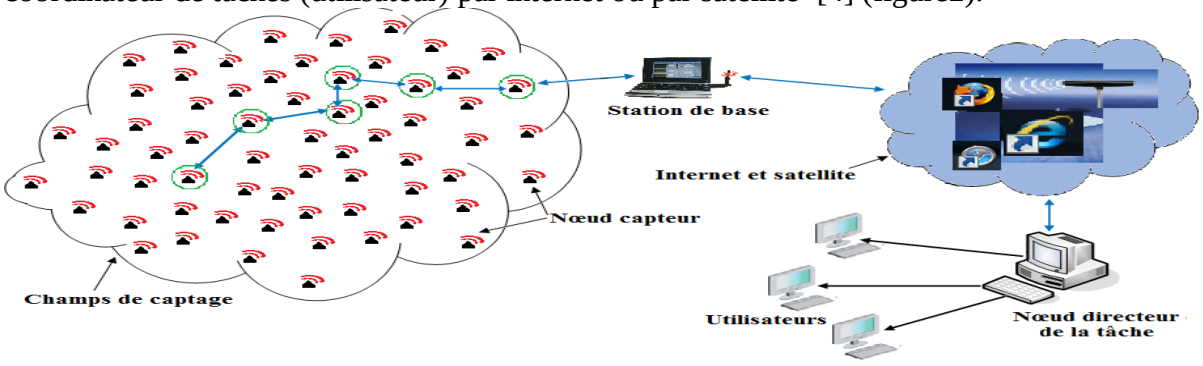


Figure 2:Architecture de communication d'un RCSF.

2.3. Domaines d'application des RCSF

La miniaturisation des micro-capteurs, le coût de plus en plus faible, la large gamme des types de capteurs disponibles (thermique, optique, vibrations, etc.) ainsi que le support de communication sans fil utilisé, permettent l'application des réseaux de capteurs dans plusieurs domaines [2] [5] parmi lesquels :

- **Domaine militaire**

Comme pour de nombreuses autres technologies, le domaine militaire a été le moteur initial pour le développement des réseaux de capteurs. Le déploiement rapide, le coût réduit, l'auto-organisation et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui font de ce type de réseaux un outil appréciable dans un tel domaine. Actuellement, les RCSFs peuvent être une partie intégrante dans le commandement, le contrôle, la communication, la surveillance, la reconnaissance, etc.

- **Domaine médical**

Les réseaux de capteurs sont également largement répandus dans le domaine médical. Cette classe inclut des applications comme : fournir une interface d'aide pour les handicapés, collecter des informations physiologiques humaines de meilleure qualité, facilitant ainsi le diagnostic de certaines maladies, surveiller en permanence les malades et les médecins à l'intérieur de l'hôpital.

- **Domaine architectural**

Transformation des bâtiments en environnements intelligents capables de reconnaitre des personnes, interpréter leurs actions et y réagir.

- **Domaine environnemental**

Dans ce domaine, les capteurs peuvent êtres exploités pour détecter les catastrophes naturelles (feux de forêts, tremblements de terre, etc.), détecter des émanations de produits toxiques (gaz, produits chimiques, pétrole, etc.) dans des sites industriels tels que les centrales nucléaires ou pétrolières.

- **Domaine commercial**

Parmi les domaines dans lesquels les réseaux de capteurs ont aussi prouvé leur utilité, on trouve le domaine commercial. Dans ce secteur on peut énumérer plusieurs applications comme : la surveillance de l'état du matériel, le contrôle et l'automatisation des processus d'usinage, etc.

2.4. Caractéristiques des RCSF

Parmi les caractéristiques les plus importantes d'un réseau de capteurs, nous citons [6] :

- ***La durée de vie limitée :*** Les nœuds capteurs sont très limités par la contrainte d'énergie, ils fonctionnent habituellement sans surveillance dans des régions géographiques éloignées. Par conséquent recharger ou remplacer leurs batteries devient quasiment impossible.

- ***Ressources limitées :*** Habituellement les nœuds capteurs ont une taille très petite, ce facteur de forme limite la quantité de ressources qui peuvent être mises dans ces nœuds. En conséquence, la capacité de traitement et de mémoire est très limitée.

- ***Topologie dynamique :*** La topologie des réseaux de capteurs change d'une manière fréquente et rapide car les nœuds capteurs peuvent être déployés dans des environnements hostiles (par exemple un champ de bataille), la défaillance d'un nœud capteur peut donc être très probable. De plus, les nœuds capteurs et les nœuds finaux où ils doivent envoyer l'information capturée peuvent être mobiles.

- ***Agrégation des données*** **:** Dans les réseaux de capteurs, les données produites par les nœuds capteurs sont très reliées, ce qui implique l'existence de redondances de données. Une approche répandue consiste à agréger les données au niveau des nœuds intermédiaires afin de réduire la consommation d'énergie lors de la transmission de ces données.

- ***La scalabilité*** : les réseaux de capteurs engendrent un très grand nombre de capteurs, ils peuvent atteindre des milliers voire des millions de capteurs. Le défi à relever par les RCFSs est d'être capable de maintenir leurs performances avec ce grand nombre de capteurs.

- ***Bande passante limitée :*** En raison de la puissance limitée, les nœuds capteurs ne peuvent pas supporter des débits élevés.

- ***Sécurité physique limitée*****:** cela se justifie par les contraintes et limitations physiques qui minimisent le contrôle des données transmises.

3. Détection d'intrusion dans les RCSF

Les réseaux de capteurs sans fil ont beaucoup d'applications potentielles. Dans beaucoup de scénarios, ces réseaux sont sujets à de nombreuses attaques en raison du déploiement en environnement ouvert et de leurs ressources limitées. Pour faire face à ces attaques des systèmes de protection existent. La détection d'intrusions peut être considérée comme une action complémentaire à la mise en place des mécanismes de sécurité.

3.1. Approches de détection d'intrusions

La détection d'intrusion peut être définie comme la détection automatique et la génération d'une alarme pour rapporter qu'une intrusion a eu lieu ou est en cours.

- **Approche comportementale :** le comportement observé du système cible est comparé aux comportements normaux et espérés. Si le comportement du système est significativement différent du comportement normal ou attendu, on dit que le système cible présente des anomalies et fait l'objet d'une intrusion [7]. L'avantage principal de cette approche est de pouvoir détecter de nouvelles attaques. Cependant, elle génère souvent de nombreux faux positifs car une déviation du comportement normal ne correspond pas toujours à l'occurrence d'une attaque.

- **Approche par scenarios** : consiste a modéliser non plus des comportements normaux, mais des comportements interdits. Dans cette approche on analyse les données d'audits à la recherche de scénarios d'attaques prédéfinis dans une base de signatures d'attaque [8]. Le principal avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit par rapport à ceux avancés par l'approche comportementale. Par contre son inconvénient majeur est de ne pouvoir détecter que les attaques enregistrées dans la base de signatures.

3.2. Propriétés des SDIs dans les RCSF

Dans les réseaux de capteurs sans fil un SDI doit satisfaire les propriétés suivantes [9] :

- ***Audit local (Localize auditing) :*** un SDI pour les réseaux de capteurs sans fil doit fonctionner avec des données d'audits locales et partielles car dans les réseaux de capteurs sans fil, il n'y a pas de points centralisés (à part la station de base) qui peut collecter les données d'audit globales.

- ***Ressources minimales (Minimize resources)***: un SDI pour les réseaux de capteurs doit utiliser un nombre minimum de ressources car les réseaux sans fils n'ont pas de connexions stables. De plus les ressources physiques du réseau et des nœuds telles que la bande passante et la puissance sont limitées. La déconnexion peut survenir à

tout moment. La communication entre les nœuds pour la détection d'intrusion ne doit donc pas prendre toute la bande passante disponible.

- ***Pas de nœud de confiance (Trust no node):*** un SDI dans les réseaux de capteur ne doit faire confiance à aucun nœud car, contrairement aux réseaux filaires, les nœuds capteurs peuvent être compromis facilement.

- ***Destribué (Be truly distributed):*** veut dire que la collection et l'analyse de données doit se faire dans plusieurs endroits (locations). De plus l'approche distribuée s'applique aussi pour l'exécution de l'algorithme de détection et la corrélation d'alertes.

- ***Sécurisé (Be secure):*** un SDI doit être capable de résister aux attaques.

3.3. Architectures des SDIs dans les RCSF

Les architectures des SDI dans les réseaux ad hoc et les réseaux de capteurs sans fils peuvent êtres classées en trois catégories [9] :

1. Stand-alone
2. Distributed and Cooperative
3. Hierarchical

- ***Autonome (Stand-alone) :*** Dans cette catégorie, chaque nœud opère comme un SDI indépendant et il est responsable de la détection des attaques contre lui. Par conséquent, dans cette catégorie, les SDI ne coopèrent pas et ne partagent aucune information entre eux. Cette architecture exige que chaque nœud soit capable d'exécuter un SDI.

- ***Distribuée et coopérative (Distributed and Cooperative) :*** Dans cette architecture chaque nœud exécute son propre SDI mais les SDIs coopèrent afin de créer un mécanisme de détection d'intrusion global.

- ***Hiérarchique* (*Hierarchical) :*** Dans ce cas le réseau de capteur est divisé en groupes (clusters). Dans chaque groupe, un leader joue le rôle de cluster-head. Ce nœud est responsable du routage dans le groupe et doit accepter les messages des membres du groupe indiquant quelque chose de malveillant. De même le cluster-head doit détecter les attaques contre les autres cluster-heads du réseau.

4. Besoin de corrélation d'alertes et choix de CRIM

La détection d'intrusions est un problème préoccupant qui vise à détecter des activités suspectes et des activités malveillantes. Deux principales approches de détection sont utilisées par les SDI . La première est l'approche comportementale qui se base sur un profil représentant les différentes activités normales au sein du système. Toute déviation par rapport

au profil établi sera interprétée comme une éventuelle intrusion. La seconde est l'approche par signatures qui consiste à vérifier les signatures d'attaques dans les données analysées. Il est clair que toute attaque qui n'a pas sa signature dans la base de signatures ne sera pas détectée, ce qui nécessite une mise à jour fréquente de la base de signatures. Ces deux approches sont indispensables pour la surveillance et la protection d'un système d'informations. En revanche, leur utilisation pose plusieurs problèmes. Le problème majeur réside dans l'excès d'alertes que les SDIs produisent. L'opérateur de sécurité qui a comme tâche d'analyser et de prendre des décisions appropriées se retrouve rapidement débordé.

4.1. Approches de corrélation d'alertes

Les trois approches de corrélation d'alertes proposées dans la littérature sont [10] [11]

- ***La corrélation implicite :*** est utilisée pour mettre en évidence des relations entre événements. Parmi les articles sur cette méthode on peut citer [11]. Cette méthode est fondée sur l'observation de groupes d'alertes et l'extraction de relations implicites entre ces alertes à travers une fonction de similarité sur les attributs. Une relation peut être constituée, par exemple, par une correspondance fréquentielle ou statistique entre des alertes. Cette correspondance est obtenue par une analyse automatique des données. Cette méthode a des limites assez rapidement, et notamment parce qu'elle ne fournit pas de relation causale entre les alertes.

- ***Corrélation explicite :*** l'opérateur est capable d'exprimer explicitement des relations entre différentes alertes, sous la forme d'un scénario. Un scénario regroupe en général un ensemble de propriétés que doivent satisfaire les alertes, et des liens les connectant. L'inconvénient de cette méthode est de nécessiter en général un expert pour fournir les scénarios d'attaques.

- ***Corrélation semi-explicite :*** Cette approche ([8] et [11]) a été développée à partir des deux précédentes afin de faire disparaître leurs inconvénients. Elle est basée sur la description logique des attaques sous la forme d'un triplet qui comprend l'attaque elle même, ses pré-conditions et ses post-conditions. Le mécanisme de corrélation consiste à corréler des alertes si les post-conditions d'une première alerte correspondent aux pré-conditions d'une alerte qui a lieu plus tard. Cette méthode permet a priori de découvrir les liens causaux entre les alertes et donc de fournir un diagnostic assez précis. De plus, la méthode semble prometteuse pour détecter les nouvelles attaques.

4.2. Description des fonctions de CRIM

CRIM [10] [11] est un module de corrélation d'alertes dans le domaine de détection d'intrusion, il intègre et implémente les six fonctions suivantes :
1- Gestion d'alertes.
2- Regroupement d'alertes.
3- Fusion d'alertes.
4- Corrélation d'alertes.
5- Reconnaissance d'intentions.
6- Réaction.

- **Fonction de gestion :** gère les alertes générées par les différents SDI en les collectant et les enregistrant dans une base de données relationnelle afin de permettre aux autres fonctions de CRIM de les analyser. Le format des alertes est supposé compatible avec celui défini par l'IDMEF [13] dont l'objectif est de fournir un format commun pour les données de détection et de permettre ainsi l'échange d'informations entre différents SDI.

- **Fonction de regroupement d'alertes :** consiste à générer des paquets d'alertes à partir des alertes de la base. Un paquet d'alertes englobe les alertes correspondant à une même occurrence d'attaque en utilisant les similarités entre les alertes.

- **Fonction de fusion d'alertes :** cette fonction prend en entrée chacun des paquets d'alertes générés par la fonction précédente, et crée une nouvelle alerte réalisant la synthèse des différentes informations contenues dans ce paquet.

- **Fonction de corrélation :** sert à analyser les alertes issues de la fonction de fusion, et de les corréler afin de reconnaître le plan d'intrusion d'un attaquant donné ; l'objectif est de détecter un attaquant qui essaye d'atteindre son objectif malveillant en lançant plusieurs attaques successives et non pas une seule attaque.

- **Fonction de reconnaissance d'intention :** les résultats de la corrélation sont des ensembles d'alertes corrélées appelés plans candidats; cependant il se peut qu'un plan candidat soit en cours d'exécution et l'objectif final de l'attaquant ne soit pas encore atteint, alors cette fonction de reconnaissance a pour but d'extrapoler le plan afin d'anticiper et de déduire les intentions de l'attaquant. Donc cette fonction doit fournir un diagnostic global de l'attaque : son passé (ce qui a été réalisé jusqu'à présent), son présent (ce que l'attaquant a obtenu et quel est l'état du système) et son futur (prévoir comment l'attaquant peut continuer son scénario d'intrusion).

- **Fonction de réaction :** cette fonction qui prend en entrée le diagnostic fourni par la fonction précédente consiste à activer une contre mesure pour stopper l'intrusion. Dans CRIM cette fonction donne à l'administration le choix de la réaction la plus adaptée.

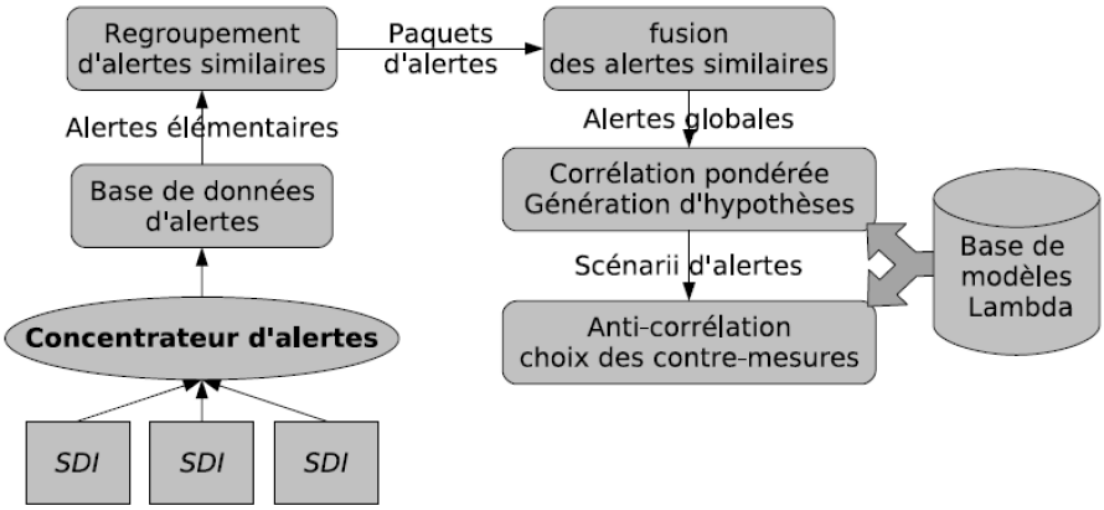


Figure 3:Architecture de CRIM

5. Architecture proposée

Dans cette section, après avoir critiqué les trois architectures de détection d'intrusion proposées pour les réseaux de capteurs sans fil, nous proposons une architecture qui tire avantage de ces dernières et limite leurs inconvénients. Cette architecture assure un double rôle de détection d'intrusion et de corrélation d'alertes dans les RCSF.

5.1. Critiques des architectures Existantes

Dans les première et deuxième architectures, chaque nœud capteur doit être capable d'exécuter un SDI : cette contrainte est très forte étant données les caractéristiques des réseaux de capteurs sans fil (énergie limitée, ressources limitées, etc.). On constate dans la première architecture une indépendance entre les différents nœuds dans le processus de détection où chaque nœud ne s'occupe que de sa protection, et ne détecte que les attaques contre lui, ce qui représente une faiblesse contre les attaques distribuées. Le problème majeur pour les SDIs de la deuxième architecture est qu'ils causent une dégradation des performances du réseau par le trafic échangé entre les différents agents SDI, en plus du gaspillage de la bande passante limitée du réseau. La dernière architecture minimise ainsi la surcharge du réseau puisque la coopération est réduite entre les chefs de groupes et leurs membres. Cependant, elle ne permet pas d'avoir une vision globale du réseau à cause de l'absence de coopération entre les différentes cellules et reste par la suite inefficace contre certaines attaques distribuées.

5.2. Description de l'architecture proposée

L'étude critique de ces trois architectures nous a permis de proposer une architecture de détection d'intrusion et de corrélation d'alertes pour les réseaux de capteurs sans fil : celle ci permet de combiner les avantages des trois approches citées précédemment et d'éliminer leurs inconvénients en exploitant l'outil de corrélation et de reconnaissance d'intentions malveillantes CRIM.

L'architecture proposée permet de faire la détection d'intrusion et la corrélation d'alertes dans les réseaux de capteurs sans fil tout en prenant en compte les caractéristiques et les contraintes très sévères de ces derniers (bande passante de réseau limitée, énergie des nœuds limitée, etc).

Notre architecture est hiérarchique : elle consiste à diviser le réseau de capteurs en zones. Dans chaque zone un nœud spécial (possédant des caractéristiques importantes) est déployé. Ce nœud, en plus des autres fonctions telles que le captage, le routage et le traitement des données; exécute un SDI qui surveille cette zone et détecte les intrusions possibles. Donc, dans notre architecture, chaque SDI a une vision locale du réseau (a accès a un ensemble de données d'audit locales spécifique à la zone dans laquelle il est déployé). Afin de faire

coopérer ces SDIs et avoir une vision globale sur les intrusions injectées dans le réseau nous relions ces SDIs avec un module de coopération et de corrélation d'alertes qui s'appelle CRIM .Ce dernier sera exécuté au niveau de la station de base : il consiste à corréler les alertes générées par les différents SDIs installés dans les différentes zones du réseau, et reconnaître les intentions des intrus impliqués en prenant en considération les informations contenues dans les alertes et en les corrélant pour détecter des relations entre les attaques individuelles pour constituer l'attaque distribuée ou le scénario d'attaques. De cette manière, nous créons un système de détection d'intrusion globale qui assure une surveillance totale du réseau.

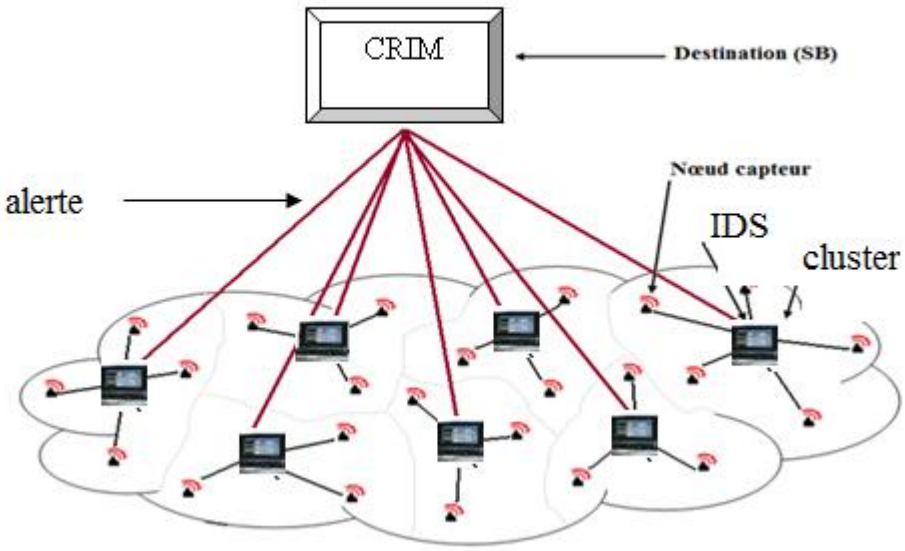


Figure 4:Architecture de détection d'intrusion et de corrélation d'alertes dans les RCSF.

5.3. Schémas de fonctionnement de l'architecture

Ce schéma représente les deux niveaux de génération d'alertes correspondant à l'architecture proposée, le niveau zone où les SDIs génèrent des alertes correspondant aux attaques élémentaires détectées, et le niveau réseau où CRIM génère des alertes synthétiques correspondant aux scénarios d'attaques.

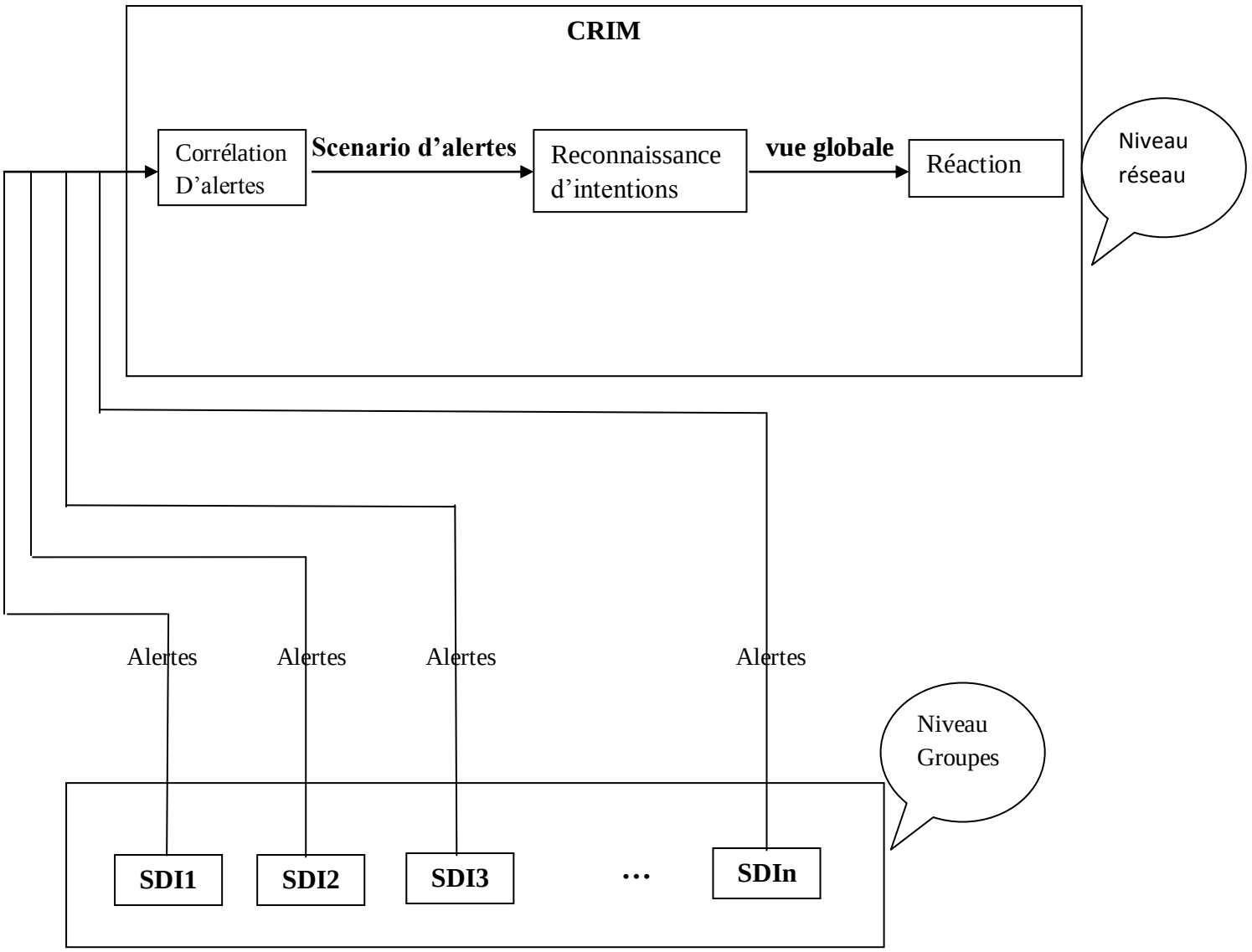


Figure 5:schéma de fonctionnement de l'architecture proposé.

5.4. Choix de CRIM

Pour faire la corrélation d'alertes dans cette architecture notre choix est porté sur le module CRIM pour les raisons suivantes :

- CRIM n'assure pas uniquement la corrélation d'alertes mais il permet aussi la réaction aux attaques.

- CRIM est développé à Télécom Bretagne, donc son code source est disponible et accessible ce qui nous permis de faire des modifications nécessaires pour son adaptation aux réseaux de capteur sans fil .

- CRIM permet d'anticiper les actions de l'attaquant en générant des hypothèses aux actions dont les alertes ne sont pas remontées par les SDIs. Cette caractéristique importante est offerte uniquement par CRIM.

5.5. Rôle de CRIM dans cette architecture

Pour répondre au besoin de corrélation d'alertes dans le domaine de la détection d'intrusion un module CRIM basée sur la troisième approche (approche semi-explicite) a été développé. Ce module fournit une base de travail intéressante pour analyser et corréler les alertes, générer un diagnostic plus global et synthétique, et aider l'administrateur de sécurité dans le choix d'une contre-mesure adaptée à l'attaque détectée. Dans notre architecture, ce module est exécuté au niveau de la station de base. Il reçoit les alertes générées par les différents SDIs installés dans les zones constituant le réseau, suite à une action suspecte ou malveillante détectée, les corrèle et génère une alerte plus globale et synthétique.

Notre objectif, derrière l'intégration de module CRIM dans notre architecture, est de garantir la couverture totale et la surveillance globale de réseau : la structuration en zone de réseaux permet aux SDIs d'avoir une vue partielle de réseau, et l'intégration de module CRIM au niveau de la station de base permet d'avoir une vue globale des intrusions impliquées. Il a pour objectifs de :

- réduire le volume d'alertes à traiter par l'administrateur de sécurité.
- réduire le nombre de faux positifs comme les alertes générées en détectant des actions suspectes.
- générer des alertes plus globales en regroupant les alertes partielles sous forme de scénarios.
- analyse plus profonde des alertes et générations des contre mesures adaptées aux scénarios d'attaques.
- création d'un système de détection d'intrusion globale sans avoir recours aux échanges entre les SDIs , ce qui permet de conserver la bande passante du réseau.
- faire la fusion des alertes au niveau de CRIM : si deux SDI de deux groupes différents détectent deux alertes différentes dont la cible est la même. Nous pouvons faire la fusion d'alertes et réduire le volume d'alertes en conséquence.
- identifier les intentions de l'attaquant, ses capacités à réussir les attaques, la cible, et le résultat final.

5.6. Conclusion

Dans cette partie nous avons proposé une architecture de détection d'intrusion et de corrélation d'alertes dans les réseaux de capteurs sans fil. Cette approche prend en compte les contraintes et les propriétés de ces réseaux. Elle combine les avantages des trois architectures proposées dans la littérature et élimine leurs inconvénients, cela à l'aide de l'intégration de module de corrélation d'alertes CRIM au niveau de la station de base.

6. Implémentation d'un scénario d'attaque dans CRIM

Dans ce qui suit, nous décrivons un scénario d'attaque dans les réseaux de capteurs sans fil et sa modélisation dans l'approche LAMBDA. C'est une attaque qui vise à épuiser la batterie d'un capteur. Les principales méthodes consistent à tromper le nœud en le maintenant éveillé, l'obligeant à écouter les communications et à retransmettre les paquets afin de consommer ses ressources et réduire sa durée de vie et celle de réseau en conséquence.

6.1. Introduction

Un réseau ne peut accomplir son objectif que tant qu'il est en vie, mais pas au delà. La durée de vie prévue est critique dans tout déploiement de réseau de capteurs. Le but des scénarios applicatifs classiques consiste à déployer des nœuds dans un domaine sans surveillance pendant des mois ou des années.

La vie d'un réseau de capteurs correspond à la période de temps durant laquelle le réseau peut, selon le cas, maintenir assez de connectivité, couvrir le domaine entier, ou garder le taux de perte d'information en-dessous d'un certain niveau. La vie du système est donc liée à la vie nodale. La vie nodale correspond à la vie d'un des nœuds du réseau. Elle dépend essentiellement de deux facteurs : l'énergie qu'il consomme en fonction du temps et la quantité d'énergie dont il dispose. La quantité prédominante d'énergie est consommée par un nœud capteur durant la détection, la communication puis le traitement des données.

À cause de la nature intrinsèque de leur fonctionnalité, les capteurs ont une contrainte principale : leur source d'énergie est limitée et presque jamais renouvelable. Ceci peut être considéré comme une vulnérabilité très importante dans les réseaux de capteurs sans fil, et les attaquants de ces derniers peuvent l'exploiter dans leur intérêt : en effet, un attaquant peut viser les nœuds les plus faibles en énergie dans le réseau et les bombarder par des rafales de requêtes en les obligeant à effectuer des traitements intenses en énergie afin d'épuiser leurs ressources et réduire leur durée de vie et celle du réseau en conséquence.

Dans ce qui suit, un scénario de cette attaque est envisagé et décrit tout en modélisant le comportement de l'attaquant et l'état de système (réseau de capteur), afin de réaliser la corrélation d'alertes et la reconnaissance d'intentions malveillantes dans les WSN en se basant sur l'approche utilisée par CRIM.

6.2. Description de scénario

Le routage multi-saut des réseaux de capteurs sans fils, a pour but d'optimiser (minimiser) la consommation d'énergie afin d'assurer une longévité maximale du réseau. Cette optimisation se fait par le choix de la route à consommation d'énergie minimale suivant :

- L'énergie disponible maximale : le choix des routes efficaces en consommation d'énergie consiste à prendre celle qui contient les nœuds possédant le maximum d'énergie totale disponible. Cette quantité est égale à la somme des énergies résiduelles des nœuds appartenant à cette route.

- L'énergie de transmission minimale : le choix se fait sur la route qui consomme le minimum d'énergie pour transmettre un paquet entre le nœud capteur et le nœud puits.

- Le nœud ayant le maximum des minimums des énergies disponibles : le choix se fait sur la route dans laquelle l'énergie disponible minimale est plus grande que toutes les autres énergies minimales disponibles sur les autres routes.

Pour cela, pour calculer les coûts des routes menant vers la station de base, un nœud ayant des données à transmettre peut être amené à solliciter l'énergie résiduelle de ses voisins. Cette dernière opération légitime peut être exploitée par un nœud malveillant à son intérêt, ce dernier peut interroger ses voisins pour récupérer leur énergie résiduelle (énergie qui peut être une métrique de routage).Cette action n'est pas dangereuse mais suspecte, car le but de l'intrus est de repérer le nœud voisin le plus faible en terme d'énergie, et le bombarder ensuite par des requêtes en lui affectant des traitements intenses et coûteux en énergie. Son but est d'épuiser les ressources de ce nœud victime (mémoire, énergie) jusqu'à sa mort et réduire en conséquence la durée de vie de réseau.

Dans ce scénario d'attaque envisagé, l'objectif de l'intrus est la réduction de la durée de vie du réseau [14].

Trois définitions de cette dernière sont présentées dans la littérature :

- **définition 1:** l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant où le premier nœud tombe énergétiquement en panne.

- **définition 2:** l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant où le dernier nœud tombe énergétiquement en panne.

- **définition 3:** l'intervalle de temps qui sépare l'instant de déploiement du réseau de l'instant où un certain pourcentage de nœuds tombe énergétiquement en panne.

Pour notre cas de scénario, nous prenons la première définition pour décrire l'objectif d'intrusion.

6.3. Hypothèses de travail

Afin d'améliorer la compréhension de notre proposition dans la suite de cette section, nous décrivons quelques hypothèses raisonnables dans le cas d'un réseau de capteurs avec une topologie sous forme de zones et avec un modèle de trafic tous-vers-un **:**

- chaque nœud capteur peut évaluer sa quantité d'énergie et la communiquer en cas de besoin.
- chaque nœud contient la liste de ses voisins à un saut après déploiement.
- Un nœud attaquant dispose des ressources suffisantes pour réaliser son attaque.
- Une fois déployés, les capteurs sont laissés sans surveillance. Il est donc impossible de les recharger en cas d'épuisement d'énergie ou de panne.
- Chaque nœud capteur a un unique identificateur connu par lui même et tous ses voisins.
- Les nœuds capteurs qui exécutent les SDIs sont un peu spéciaux (possèdent des ressources importantes).
- Afin de faire la corrélation des alertes au niveau de CRIM, les SDIs doivent être capables de détecter différents types d'attaques (impliqués dans les scénarios).

6.4. Plan de l'intrusion

Le comportement de l'attaquant réalisant l'intrusion dans le système (réseau de capteurs) est représenté par un plan d'intrusion. Un plan d'intrusion est composé d'un ensemble d'actions permettant à l'attaquant de progresser dans le système : ces actions sont les attaques (actions suspectes, action malveillantes), correspondant à l'exploitation d'une vulnérabilité du système. Certaines attaques peuvent être corrélées, par exemple quand la réalisation d'une attaque permet d'en effectuer une deuxième. Chaque plan correspond à un ensemble d'attaques cohérentes qui peuvent être corrélées. A un moment donné du déroulement de l'intrusion, ce plan est partiellement réalisé par l'attaquant. Dans ce qui suit les étapes de l'intrusion décrite dans l'introduction sont détaillées.

Etape 1: récupération d'énergie résiduelle des nœuds voisins

Dans cette étape, l'intrus essaye de prendre connaissance de son voisinage en interrogeant ses voisins afin de récupérer leur énergie résiduelle (énergie résiduelle des voisins peut être une métrique de routage, elle peut être utilisée pour choisir le prochain saut dans les protocoles de routage) donc cette action est une action légitime mais elle est suspecte car elle peut être une étape pour exécuter une action malveillante dans le scénario suivi par l'intrus.

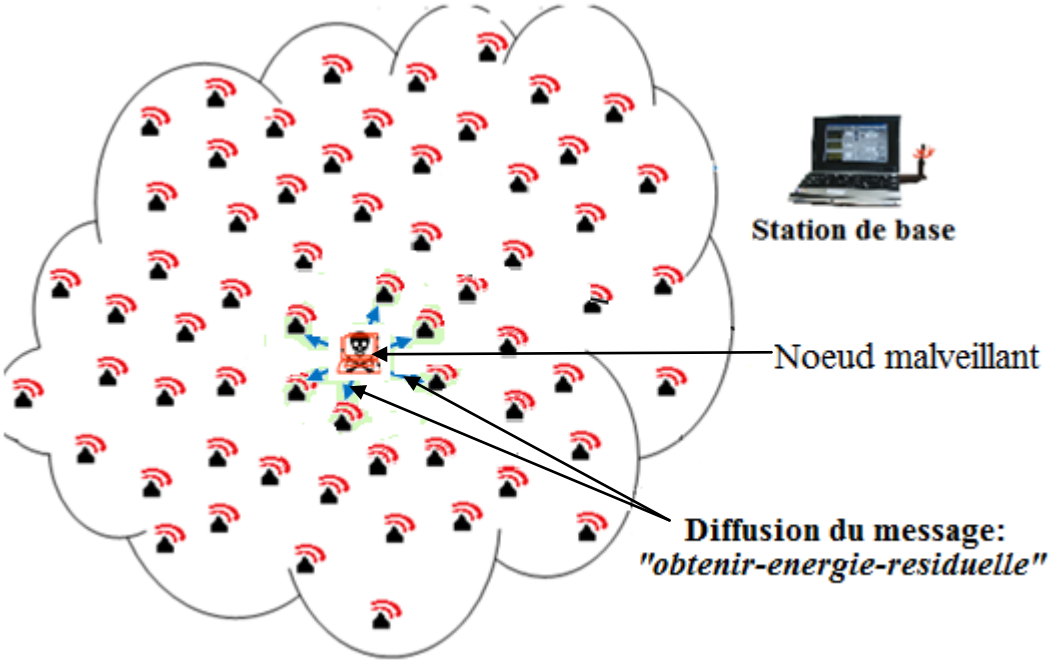


Figure 6:Sollicitation d'énergie résiduelle des voisins par l'attaquant

Etape 2: traitement local par l'attaquant et repérage du nœud le plus faible dans le voisinage

Une fois que l'attaquant a récupéré les énergies résiduelles de ses voisins dans l'étape précédente, il fait des traitements locaux pour repérer le nœud voisin le plus faible en énergie et récupérer sa localisation géographique en conséquence. Dans cette étape, l'attaquant classe les nœuds voisins selon leur énergie résiduelle et récupère-les cordonnées du nœud voisin visé par l'attaque qui possède une quantité d'énergie minimale pour qu'il soit la cible de l'action suivante. Pour cette étape, aucune alerte ne sera générée par les SDI car c'est une action locale de l'attaquant. Cependant comme CRIM anticipe les actions de l'attaquant, il génère une hypothèse correspondant à cette étape.

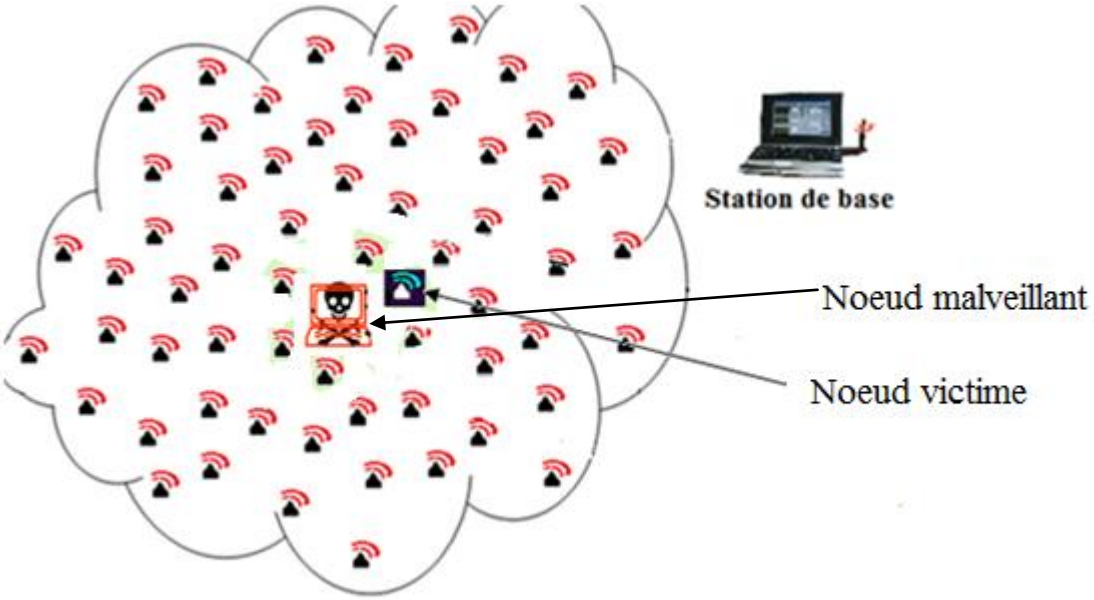


Figure 7:l'attaquant a repéré le nœud victime.

Etape 3 : bombardement du nœud victime par des requêtes

Cette étape est la dernière du scénario envisagé : elle consiste à bombarder le nœud victime par des requêtes légitimes afin de l'empêcher d'être en mode « **sleep**» en lui affectant des traitements intenses en énergie jusqu'à sa mort.

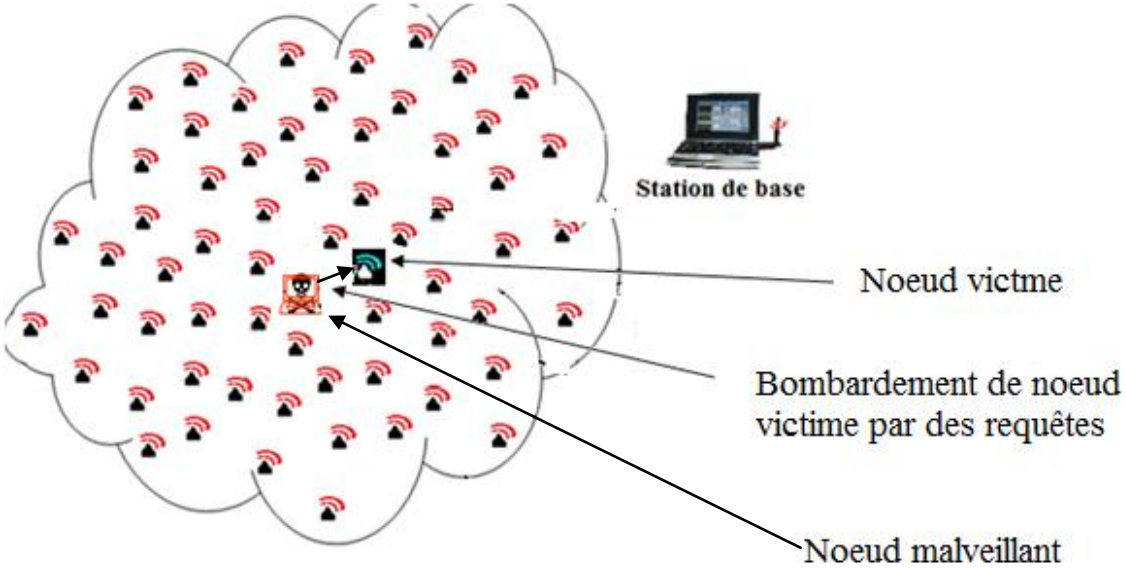


Figure 8:bombardement du nœud victime par des requêtes

Cette attaque peut être classée comme une attaque de « **sleep deprivation attack** » par définition. La privation de mise en veille a pour but de consommer toutes les ressources de la victime en l'obligeant à effectuer des calculs ou à recevoir ou transmettre des données inutilement. Dans notre cas, nous modélisons l'objectif de l'intrus comme étant la réduction de durée de vie du réseau.

6.5. Modélisation de l'intrusion dans CRIM

Cette section consiste à modéliser le scénario décrit dans la section précédente dans l'approche CRIM.

En général un attaquant doit réaliser plusieurs actions, organisées en un scénario d'intrusions, afin d'arriver à atteindre ses objectifs. Nous représentons ces actions dans CRIM par leurs pré-conditions et post-conditions qui correspondent à un ensemble de prédicats logiques ou de négation de prédicats. La pré-condition d'une action représente l'état dans lequel doit être le système afin de pouvoir exécuter l'action. La post-condition correspond aux effets de l'exécution de l'action sur l'état du système (réseau de capteurs).

- **Description des prédicats**

Prédicats	**Signification**
neighbor (N, V):	le nœud capteur V est voisin du nœud capteur N
state (N, Etat)	le nœud capteur N est dans l'état donné par la variable etat
energy (V, E)	le nœud capteur V a la quantité d'énergie E
energy_min_neighbor(V)	Le nœud voisin V a le minimum d'énergie
target(Attacker,V):	le nœud voisin V est la cible de l'attaquant Attacker
knows(Attacker,predicat)	Connaissance de l'attaquant du prédicat

Tableau 1: prédicats représentant l'état de RCSF.

- **Description des attributs**

Name	**Type**	**Description**	**Exemple**
N, V, Attacker	Adresse	Les cordonnées des nœuds capteurs	1, 21,32
Etat	String (énuméré)	Etat d'un nœud capteur	Sleep ,dead, idle,actif
E	Float	Energie résiduelle d'un nœud capteur	1.5

Tableau 2: Attribut représentants les variable des modéles.

- **Valeurs de la variable etat**

Rang	Mot clés	Signification
1	sleep	le nœud capteur est en veille
2	idle	il est seulement à l'écoute d'éventuels messages à recevoir
3	actif	il exécute une fonction ou transmet un message, en mode actif le capteur peut envoyer et recevoir des messages.
4	dead	le nœud capteur est en panne car sa batterie est vide.

Tableau 3: valeurs de la variable état.

6.6. Modèles Lambda de scénario

Dans CRIM, l'approche de corrélation utilisée est l'approche semi-explicite. Elle est basée sur la description logique des attaques dans le langage LAMBDA[15]. Dans ce langage, une attaque est spécifiée en utilisant les attributs suivants :

– La pré-condition : condition logique qui spécifie les conditions qui doivent être satisfaites pour que l'attaque soit un succès.

– La post-condition : condition logique qui spécifie les effets de l'attaque lorsque l'attaque est un succès.

– La détection : mise en correspondance d'un modèle LAMBDA et une alerte et instanciation des variables du modèle.

– La vérification : combinaison d'événements qui permet de vérifier que l'attaque est un succès.

Par la suite, une analyse est faite pour étudier les liens logiques entre la post-condition d'une attaque A et la pré-condition d'une attaque B. Si un tel lien existe, l'attaque A a été faite dans le but de faire ensuite l'attaque B. Dans cette approche, les différents liens logiques sont automatiquement découverts au cours d'une phase d'analyse préalable de la base d'attaques spécifiées en LAMBDA. Ceci permet de générer une base de règles de corrélation qui sont ensuite appliquées pour corréler les alertes et construire des plans d'intrusions candidats correspondant à l'activité de l'attaquant. Pour prendre en compte des alertes spécifiques aux réseaux de capteurs sans fil, l'extension de modèle IDMEF est nécessaire (voir la sous section 6.8).

Dans ce qui suit, nous décrivons le plan d'intrusion discuté auparavant dans le langage Lambda.

Nom de l'action	**Preconditions**	**Postconditions**
remaining_energy_neighbors	neighbor(Attacker,V) not(state(V,sleep)) ,energy(V,E)	knows(Attacker,energy(V,E))
target_spoted	energy(V,E) , energy_min_neighbor(V)	target(Attacker,V)
energy_request_flooding	target(,Attacker,V) , not(state(V,sleep))	state(V,dead)
Put_to_sleep	energy(V,E), inf(E,seuil)	state(V,sleep)

Tableau 4:récapitulatifs des pré-conditions et post conditions des actions.

6.6.1. Les actions

- **Model 1 remaining_energy_neighbors**

Le model 1 représente l'étape 1 de l'intrusion envisagé en utilisant le langage lambda

```
<action>
<name> remaining_energy_neighbors        </name>
<pre> neighbor(Attacker,V) , not(state(V,sleep)) , energy(V,E) </pre>
<post> knows(Attacker,energy(V,E))</post>
<detection> Attacker=//Source/Node/Geographical_localization/text(),
              V=//Target/NOde/Geographical_localization/text(),
             classification=ACTION1
 </detection>
</action>
```

- **model 2 target_spoted**

Ce model correspond à l'étape 2 de l'intrusion**.**

```
<action>
<name>  target_spoted </name>
<pre> energy(V,E) , energy_min_neighbor(V)</pre>
<post> target(Attacker,V) </post>
<detection> V=//Target/Node/Geographical_localization/text(),
              classification=ACTION2
</detection>
</action>
```

- **Model 3 energy_request_flooding**

Le modèle 3 représente la troisième et dernière étape du plan de l'intrusion, il montre l'attaque réelle planifiée par l'attaquant **:**

```
<action>
<name>  energy_request_flooding  </name>
<pre>  target(V) , not(state(V,sleep))  </pre>
<post>  state(V,dead)  </post>
<detection>  V=//Target/Node/Geographical_localization/text(),
        classification=ACTION3
 </detection>
</action>
```

6.6.2. Objectif de l'intrusion

Un objectif d'intrusion représente l'état de système dans lequel une anomalie dans le système est présente .Cet état est spécifié par une condition logique : dans notre cas, il suffit que le premier nœud du réseau tombe en panne pour dire que l'objectif de l'intrusion est atteint, c'est-à-dire que la durée de vie du réseau est réduite par cette intrusion **«reduce_network_life»**.
L'objectif d'intrusion dans ce scénario est représenté par le modèle suivant :

- **modèle 4 Objectif d'intrusion "reduce_network_life"**

<objective>
<name> **reduce_network_life** </name>
<condition> state(V,dead) </condition>
</objective>

6.6.3. Reconnaissance d'intention et réactions

La réalisation du scénario décrit ci-dessus permet à un attaquant d'atteindre un objectif d'intrusion **«reduce_network_life»** qui correspond à la réduction de la durée de vie de réseau. La fonction de reconnaissance d'intentions est utilisée pour détecter que l'objectif d'intrusion est atteint. Une possibilité de contre mesure consiste à réagir avant que l'objectif d'intrusion ne soit atteint : par exemple, la contre mesure «**no_repense**» qui ferme la connexion avec l'attaquant et qui consiste à ne pas répondre aux requêtes de l'attaquant est une contre mesure candidate.

Dans cette contre mesure, si l'intention de l'attaquant est reconnue, une réaction est générée avant que le réseau soit remis en cause.

Au niveau réseau de capteurs, la réaction consiste à envoyer un message d'alerte de la station de base vers les nœuds cluster-head qui exécutent les SDIs. Ces nœuds, à leur tour, transmettent le message vers les nœuds appartenant à la zone. A la réception de ce message d'alerte, chaque nœud du réseau bloque ses communications avec l'attaquant, y compris le nœud victime. De cette façon, il conserve son énergie restante pour d'autres fonctions telles que le captage, etc. En conséquence, l'objectif d'intrusion ne sera pas atteint car son intention est reconnue et une réaction est activée au bon moment.

- **modèle 5 : modèle de réaction "put_to_sleep"**

Au niveau du module CRIM, nous nous basons sur l'énergie résiduelle des nœuds capteurs pour définir la réaction. Le modèle 5 ci –dessous représente l'action de réaction menée par CRIM pour stopper l'intrusion**.** Elle consiste à vérifier le prédicat **inf (E,seuil)**. Ce prédicat est vrai si l'énergie résiduelle de la victime V est inférieure au seuil prédéfini. Si c'est le cas, alors l'état du nœud attaqué sera mis en mode sleep afin d'anti-corréler la dernière étape du plan de l'intrus pour que la pré-condition de la troisième étape du scénario ne soit pas vérifiée, et l'attaque sera arrêtée en conséquence avant que l'objectif de l'intrusion ne soit atteint.

<action>
<name> **put_to_sleep** </name>
<pre> energy(V,E),inf(E,seuil) </pre>
<post> state(V,sleep) </post>
</action>

6.7. Schéma de corrélation d'alertes

La figure suivante représente le schéma de corrélation d'alertes dans le scénario précédant ; il résume le comportement de l'attaquant et l'état de système (réseau de capteurs) .

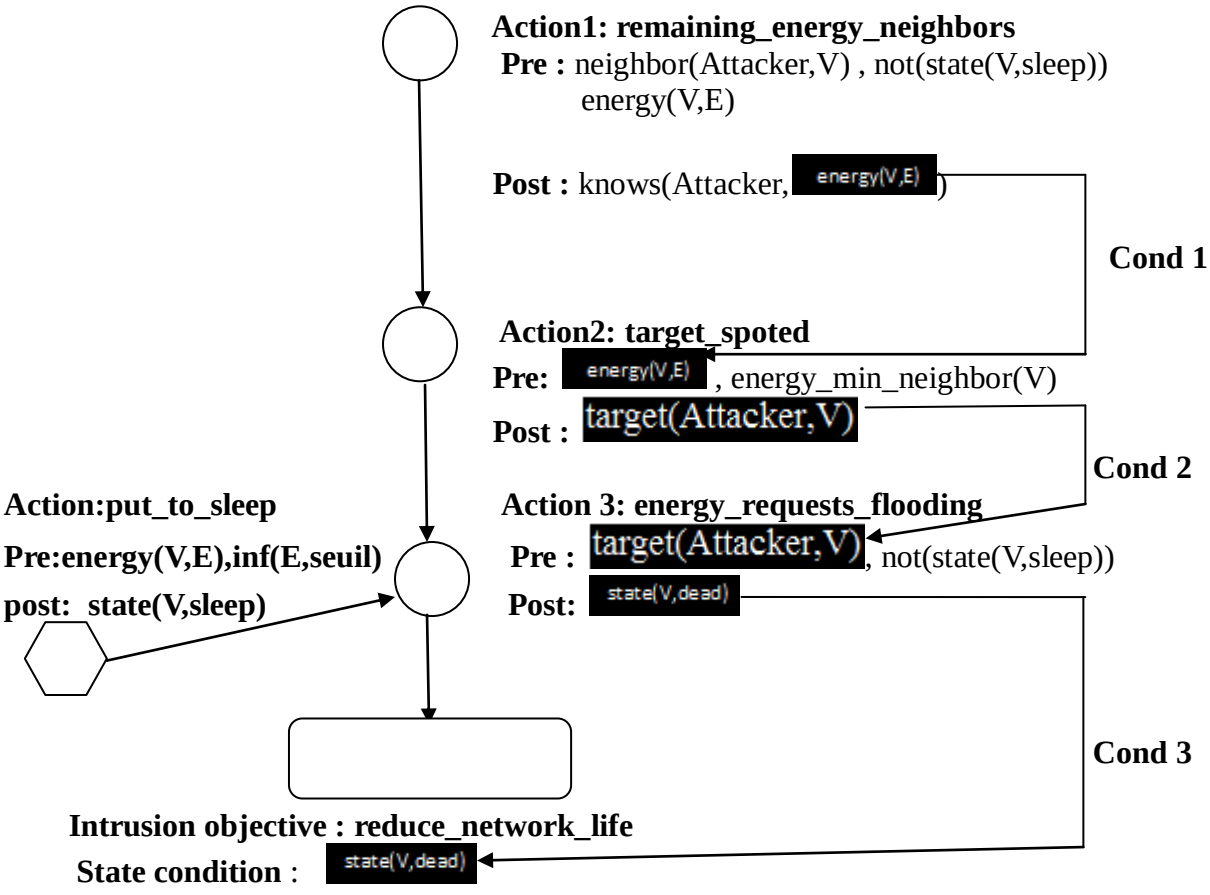


Figure 9:graphe de corrélation d'alertes dans le scénario

6.8. Implémentation et mise en ouvre dans CRIM

Ce travail est le premier travail concernant la corrélation d'alertes dans les réseaux de capteurs en utilisant CRIM. Dans notre implémentation, nous avons construit une base de travail qui pourra être enrichie et améliorée dans les futurs travaux pour implémenter des scénarios plus complexes :

Le schéma suivant représente l'arboressence des fichiers créés afin d'implémenter le scenario décrit ci-dessus

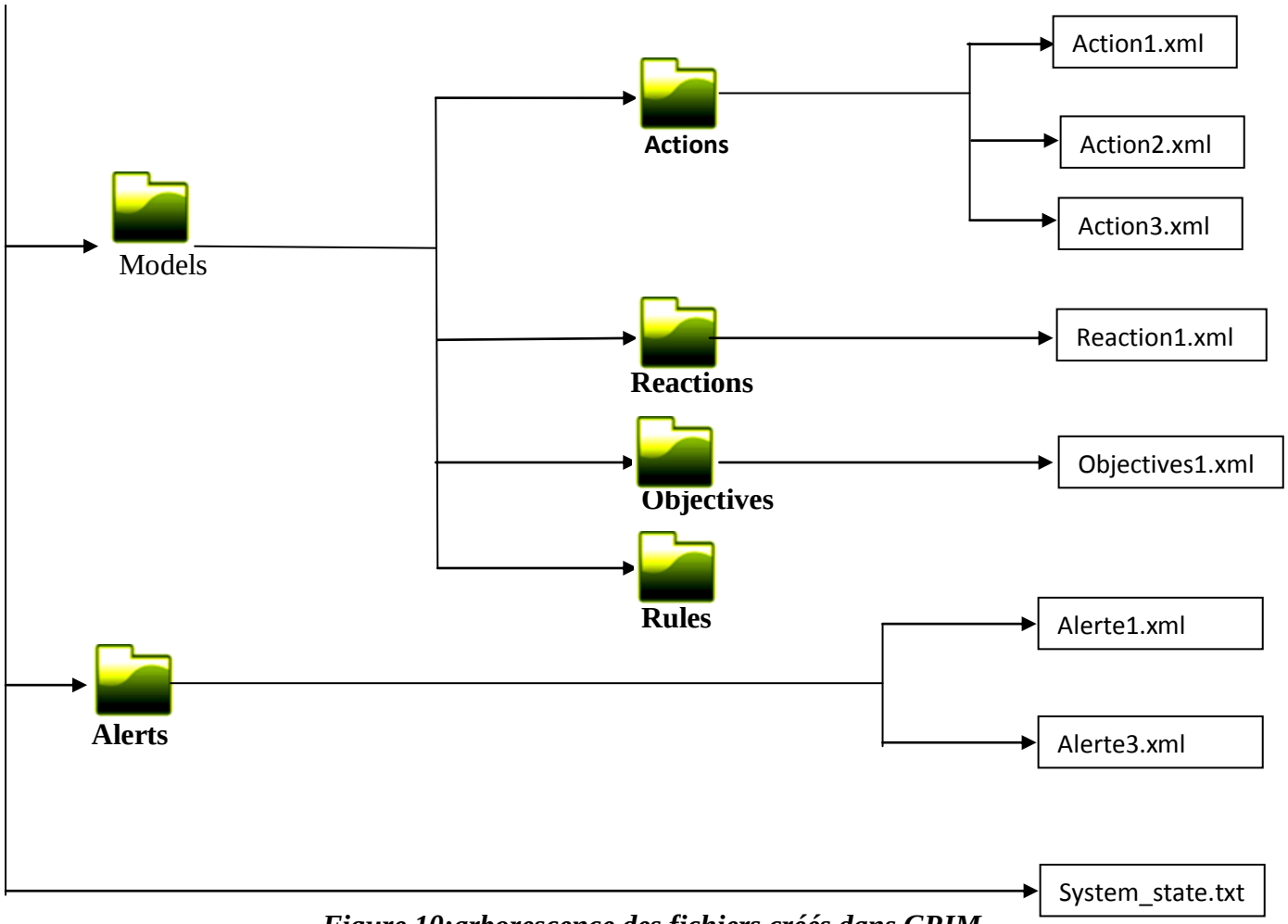


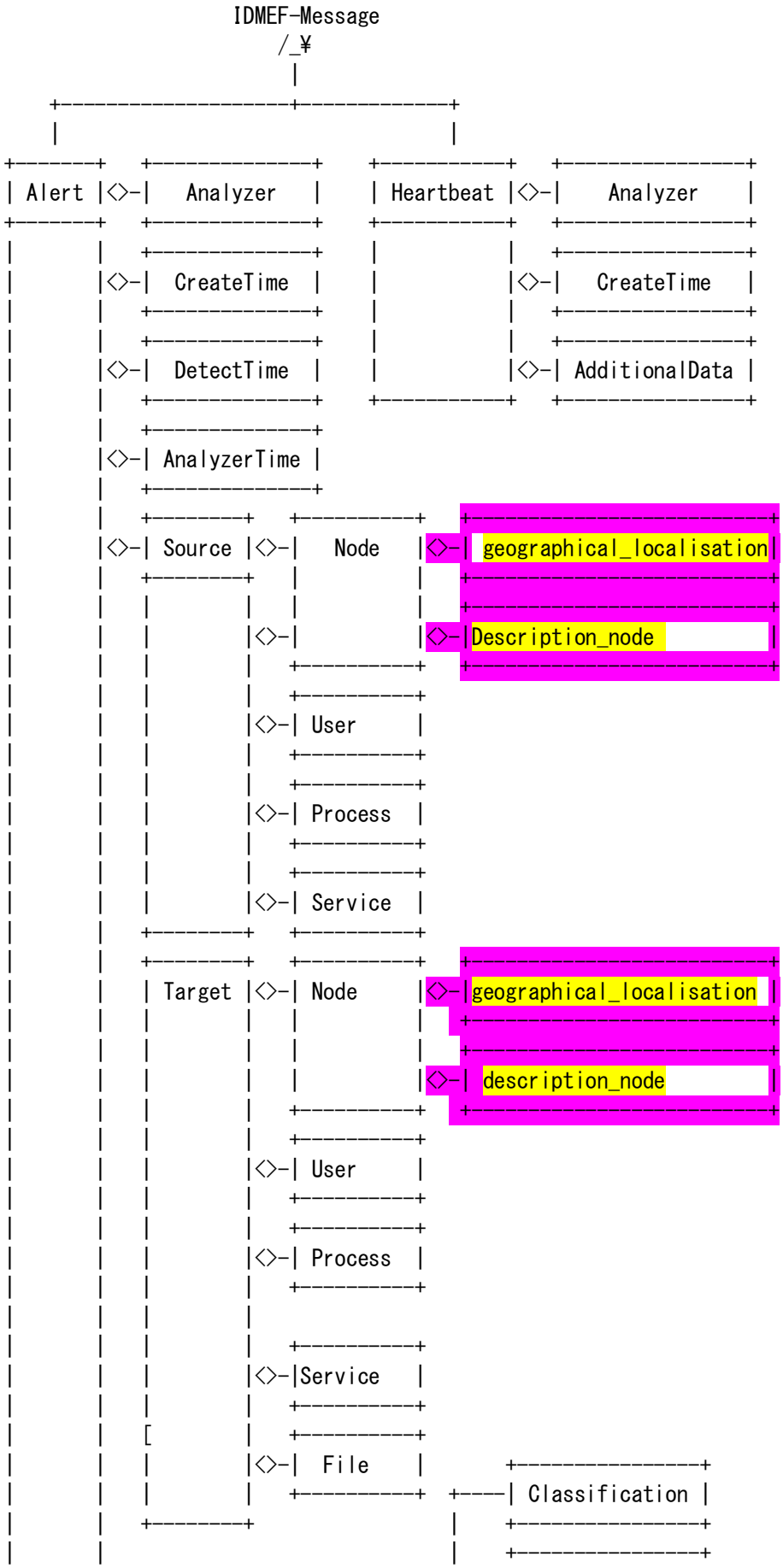
Figure 10:arborescence des fichiers créés dans CRIM

Afin d'adapter CRIM pour ce genre de réseaux, de nouvelles intégrations doivent êtres ajoutées.

- construction d'une base des faits qui contient les différents prédicats qui spécifient les caractéristiques des nœuds capteurs (état de son module radio comme sleep, idle, etc, son niveau d'énergie).

- extension du modèle IDMEF pour prendre en compte les alertes spécifiques aux réseaux de capteurs sans fil.
  - comme dans les réseaux de capteur sans fil, l'adressage n'est pas un adressage IP, les nœuds capteurs sont repérés par leurs cordonnées géographiques : alors une classe agrégée de la classe Node dans le format IDMEF est ajoutée. Cette classe qui a été nommée Geographical_localization consiste à associer à chaque nœud capteur des cordonnées sur les trois axes (X, Y, Z).
  - de même pour décrire les caractéristiques d'un nœud capteur, une classe Description_node est ajoutée comme une classe agrégée de la classe Node : cette classe sert à décrire les propriétés d'un nœud capteur, à savoir son énergie résiduelle et son état qui prend les valeurs sleep, idle , dead, actif.

La figure suivante montre l'organigramme du format IDMEF après extension


IDMEF-Message
Alert
Analyzer
CreateTime
DetectTime
AnalyzerTime
Source
Node
User
Process
Service
Target
Node
User
Process
Service
File
Heartbeat
Analyzer
CreateTime
AdditionalData
geographical_localisation
Description_node
geographical_localisation
description_node
Classification

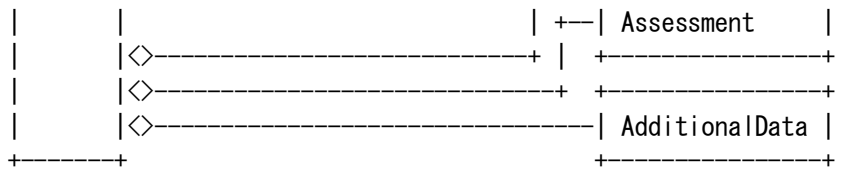


Figure 11:format IDMEF après extension.

Exemples d'alerte generé par un SDI

```
<?xml version="1.0" encoding="UTF-8"?>
  <idmef:IDMEF-Message version="1.0"
                xmlns:idmef="http://iana.org/idmef">
<idmef:Alert messageid="01">
      <idmef:Analyzer analyzerid="01">
      </idmef:Analyzer>
      <idmef:CreateTime ntpstamp="0xc56b24dc.0x6b7d9557">2004-12-
15T21:02:20Z</idmef:CreateTime>
      <idmef:Source >
        <idmef:Node >
          <idmef:Geographical_localization  > 10.10.0 </idmef:Geographical_localization >
           <idmef:Description_node  > </idmef:Description_node>
        </idmef:Node>
      </idmef:Source>
      <idmef:Target >
        <idmef:Node>
          <idmef:Geographical_localization > 10.11.0 </idmef:Geographical_localization  >
          <idmef:Description_node residual_energie ="0.6",state ="actif" >
          </idmef:Description_node>
        </idmef:Node>
      </idmef:Target>
 <idmef:Classification text="Energy residuelle neighbors">
   <name>ACTION1</name>
 </idmef:Classification>
    </idmef:Alert>
  </idmef:IDMEF-Message>
```

Figure 12:exemple d'alerte.

Le graphe suivant montre l'avancement de l'attaquant dans son scénario, il montre que l'attaquant a réalisé l'action 1 du scénario ; l'action1 entouré d'un cercle en noir dans le graphe signifie qu'une alerte de détection de l'action 1 est remontés vers CRIM

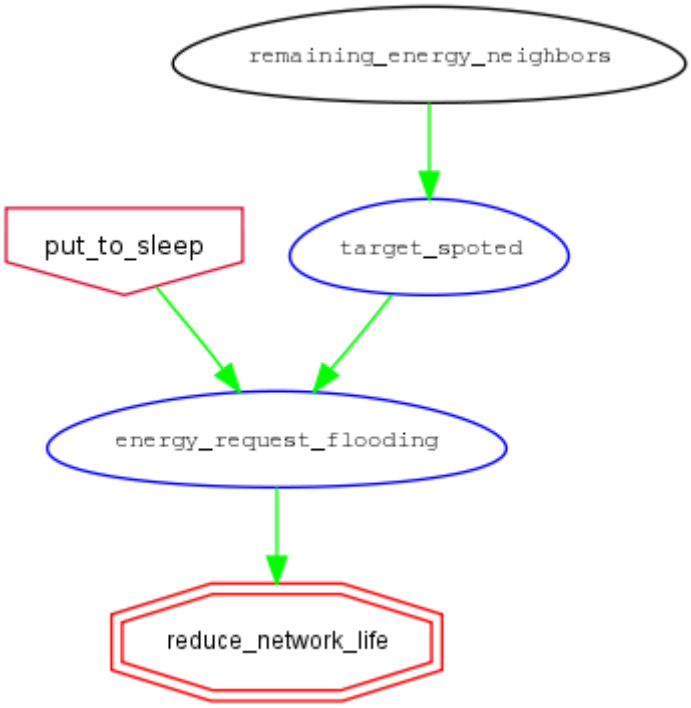


Figure 13:scenario d'attaque dans les RCSF.

Après réception des deux alertes alerte1.xml et alerte3.xml qui correspondent aux deux actions action1 et action3 ; CRIM réalise la corrélation d'alerte et génère une alerte synthétique correspondante au scénario complet décrit auparavant.

7. Perspectives et scénarios complexes

En général, un attaquant essaye d'atteindre un certain objectif en lançant plusieurs attaques successives, et non pas une seule attaque. Ces attaques successives constituent des plans d'intrusion. En effet, l'attaquant lance ses attaques dans l'ordre. Chacune lui permet d'exécuter la prochaine étape afin de réaliser son objectif malveillant. Etant donné qu'il existe des relations de plausibilité entre les différentes attaques, leur corrélation dans des scénarios d'attaques est nécessaire. Dans ce qui suit, nous proposons un schéma représentant des attaques qui peuvent êtres corrélées dans des scénarios dans les réseaux de capteurs sans fil.

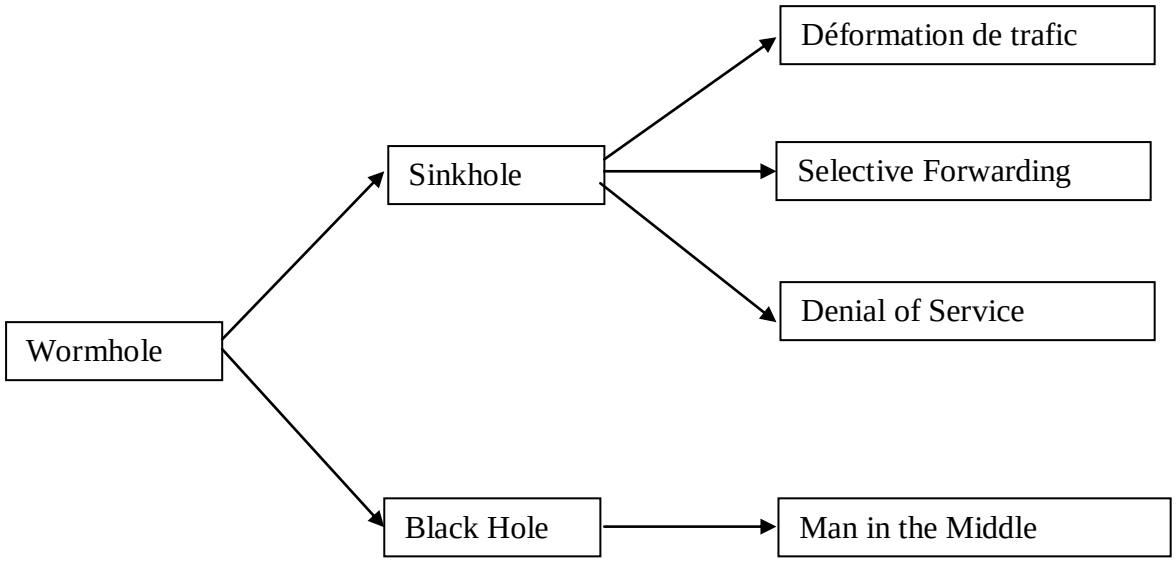


Figure 14:scénarios complexes

La figure 14 presente un scénario d'attaques complexe. L'attaque ***Wormhole***[16][17] est une attaque radio qui consiste à utiliser une fréquence hors bande pour router les données. En réussissant cette attaque, le nœud malveillant va bénéficier de ce chemin en dehors du réseau pour exécuter l'attaque ***Sinkhole***[16][17] qui vise à attirer à lui-même les données de tous ses voisins. Ainsi, il peut appliquer l'attaque "**Déformation du trafic**" pour fureter le trafic du réseau, manœuvrer ou corrompre le contenu des paquets ou bloquer certains types de trafic. Il peut faire aussi l'attaque ***Selective Forwarding***[17[18] en refusant d'envoyer certains messages et les ignorer.

A travers de cette attaque radio, l'attaquant peut lancer l'attaque *Black Hole* en s'annonçant comme un nœud ayant le chemin le plus court. Et par la suite, il peut surveiller et analyser le trafic de tous ses voisins pour trouver leurs modèles d'activités (***Man in the Middle***).

8. Bilan

Les réseaux de capteurs sans fil sont en plein développement, et deviennent de plus en plus répandus. Actuellement, ils constituent un thème de recherche très dynamique, tiré vers le haut, par leurs utilisations dans divers domaines. En effet, leurs applications sont de plus en plus nombreuses et diversifiées. Une problématique majeure dans les réseaux de capteurs, est leur sécurité. En effet ces derniers sont très vulnérables à de multiples attaques vu leur contraintes critiques (énergie, mémoire, etc.).

Dans ce travail, nous nous sommes intéressés à la problématique de sécurité dans les réseaux de capteurs sans fil. Plus précisément à la détection d'intrusion et la corrélation d'alertes dans ces derniers.

Notre contribution consiste en une étude critique des trois architectures de détection d'intrusion proposées pour les réseaux de capteurs sans fil. Nous avons contribué par la proposition d'une architecture qui combine les avantages et élimine les inconvénients de ces trois architectures proposées dans la littérature. Elle assure un double rôle : la détection d'intrusion et la corrélation d'alertes, grâce à l'intégration du module CRIM au niveau de la station de base. Un scénario d'attaques et sa modélisation dans le langage LAMBDA a été détaillé dans ce rapport. Comme perspectives de ce travail, nous avons proposé un schéma détaillant des attaques qui peuvent être corrélées en des scénarios plus complexes.

Nous voudrions évaluer les performances de notre architecture et les comparer avec les trois architectures existantes dans la littérature. Pour cela nous avons manipulé le logiciel de simulation omnet++ [19]. Nous avons appris à modéliser des réseaux avec ce logiciel et les configurer. Cependant vu la contrainte de temps nous n'avons pas pu terminer cette évaluation ; pour cela nous envisageons aussi comme perspective de notre travail l'évaluation de performance de notre architecture.

9. Conclusion Générale

Ce projet nous a permis de toucher à la réalité du travail dans un laboratoire de recherche. Nous avons appris à considérer les notions d'un œil critique afin de vouloir toujours améliorer, toujours essayer de changer et d'innover. Cette expérience est la première dans notre jeune formation, et elle fût réussie à plusieurs points de vue. Sur le plan concret, ce projet nous a offert l'occasion de travailler sous l'environnement Linux, découvrir l'outil de corrélation d'alerte CRIM, et l'outil de simulation des réseau omnet++, découvrir des domaines de recherches très récents, à savoir les réseaux de capteurs, la détection d'intrusion, et la corrélation d'alertes. Cette aventure de recherche nous a permis de bien travailler en équipe au sein de l'équipe SERES, et de développer nos compétences en termes de rigueur, esprit d'équipe, créativité, gestion de projet.

Le travail réalisé s'est avéré très intéressant et très enrichissant pour mon expérience professionnelle. En effet, ma formation s'inscrit précisément dans ce secteur (sécurité des infrastructures et des contenus informatiques). Grâce à ce stage, j'ai travaillé sur des sujets qui m'ont permis d'entrevoir en quoi consiste la profession d'un chercheur dans ce secteur d'activité.

Résumé

Mot clés : Réseaux de capteurs, détection d'intrusion, corrélation d'alertes, CRIM

Le présent rapport a été élaboré dans le cadre du projet de fin d'études pour l'obtention du diplôme de master en informatique. Ce travail consiste à proposer une architecture de détection d'intrusion et de corrélation d'alertes dans les réseaux de capteurs sans fil. Elle consiste à adapter le module de corrélation d'alertes CRIM dans le domaine de la détection d'intrusion dans les réseaux de capteurs sans fil.

Abstract

Keywords: sensors' networks, detection of intrusion, correlation of alerts, CRIM

The present report (relationship) was elaborated within the framework of the project of the end of studies for obtaining the Master's degree in computing. This work consists in proposing architecture of detection for intrusion and correlation of alerts in wirless sensors' networks. It consists in adapting the module of correlation of alerts CRIM in the field of detection of intrusion in wireless sensors' networks.

Références Bibliographiques

[1] I.F. AKYILDIZ, W. S. SANKARASUBRAMANIAM, E. CAYIRCI : Wireless Sensor Networks: A Survey. Computer networks, 2002, 38, pp. 393-422.

[2] David Culler, Deborah Estrin, and Mani Srivastava. Guest editors' introduction : Overview of sensor networks. Computer, 37(8) :41-49, August 2004. 5, 6

[3] P. MOHAPATRA, S. V. KRISHNAMURTHY: Ad Hoc Networks Technologies and Protocols. Springer Verlag Telos, 2004, ISBN: 0-387-22689-3.

[4] I. Akyildiz, W. Su, E. Cayirci, Y. Sankarasubramaniam. A survey on sensor Networks. IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Georgia Institute of Technology, Atlanta, USA. Août 2002.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. l. Cayirci. A survey on sensor Networks. IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-116, Août 2002.

[6] A. Delye, V. Gauthier, M. Marot, and M. Becker. Etat de l'art sur les réseaux de capteurs. Rapport de Recherche INT N-05001RST GET-INT, UMR5157 SAMOVAR, Institut National des Télécommunications, Evry, France, 2005.

[7] Messai Mohamed Lamine. Securite dans les Reseaux de Capteurs Sans-Fil. Memoire de Magistere en Informatique Ecole Doctorale d'Informatique de bejaia 2007/2008.

[8] Peng Ning ,Yun Cui,and Douglas S .Reeves. Construc-ting attacks scenarios through correlation of intrusion alerts. In ACM Conference on Computer and Comminication Security.pages 245-254,2002.

[9] Andreas A. Strikos. A full approach for Intrusion Detection in Wireless Sensor Networks. School of Information and Communication Technology KTH Stockholm,

[10] Fabien Autrel et Frédéric Cuppens. CRIM : un module de corrélation d'alertes et de réaction aux attaques. Annals of Telecommunications.Vol. 61.no. 9-10.Septembre-octobre 2006.

[11] Frédéric Cuppens and Alexandre Miége.Alerte correlation in a cooperative intrusion detection framework.In IEEE Symposium on Security and Privacy pages 202-215,2002.

[12] Frédéric Cuppens .Managing alerts in a multi-intrusiondetection envirenement .In ACSAC,pages 22-31,2001.

[13] Curry (D.), Debar (H.), Intrusion Detection Message Exchange For-mat Data Model and Extensible Markup Language (XML) Document Type Definition, draft-itetf-idwg-idmef-xml-14.txt, Janvier 2005.

[14] R.KACIMI .Techniques de conservation d'énergie pour les réseaux de capteurs sans fil. Thèse de doctorat .université de Toulouse Ecole doctorale : Mathématiques Informatique et Télécommunications Unité de recherche : IRIT .2009.

[15] Frédéric Cuppens and Rodolphe Ortalo. Lambda : A language to model a database for detection of attacks. In Recent Advances in Intrusion Detection, pages 197-216, 2000.

[16] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols , 1(2_3):293_315, September 2003.

[17] Wassim Znaidi,Marine Menier Jean-Philippe Babau. An Ontology for Attacks in Wirless Sensor Networks. INSTITU NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE N° 6704 Octobre 2008.

[18] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, 1(2-3):293–315, August 2003.

[19] András Varga. Using the OMNeT++ Discrete Event Simulation System in Educa tion. IEEE Transactions on Education, 42(4):372, November 1999. (on CD-ROM issue; journal contains abstract).